UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

SARAH SMITH, individually and on behalf of all others similarly situated, *Plaintiff*, vs. **GRYPHON HEALTHCARE, LLC** *Defendant*.	)	Case No. 4:24-cv-3968

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT

Plaintiff, SARAH SMITH ("Plaintiff") brings this Class Action Complaint ("Complaint") against GRYPHON HEALTHCARE, a Limited Liability Company, ("Gryphon" or "Defendant"), for its failure to properly secure and safeguard Plaintiff's and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including without limitation, names, Social Security numbers, dates of birth, health plan information, and medical information (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI" and "personally identifiable information" or "PII").

Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of counsel, and facts that are a matter of public record.

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant, Gryphon.

2. Plaintiff further seeks to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part

164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

3. On information and belief, on or around August 13, 2024, Gryphon became aware of a data security incident involving a partner that Gryphon provides medical billing services for, which resulted in unauthorized access to certain personal and/or protected health information maintained by Gryphon, resulting in the unauthorized disclosure of the Personal Information of Plaintiffs and the Class Members, including names, dates of birth, patient records, Social Security numbers, and other PHI (the "Data Breach").

4. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Gryphon, and the resulting misuse of their Personal Information and fraudulent activity, including monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals because of the tortious conduct of Defendant.

5. On behalf of themselves and the Class preliminarily defined below, Plaintiff brings causes of action for: (i) Negligence and Negligence *Per Se*; (ii) Implied Breach of Contract; (iii) Breach of Fiduciary Duty; (iv) Intrusion Upon Seclusion/Invasion of Privacy; (v) Unjust Enrichment and (vi) Declaratory Judgment and Injunctive Relief. Plaintiff seek damages and injunctive and declaratory relief arising from Gryphon's failure to adequately protect their highly sensitive Personal Information.

NATURE OF THE ACTION

6. Plaintiff brings this class action lawsuit against Defendant, Gryphon for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former Defendant clients' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, addresses, dates of birth, phone numbers, Social Security numbers, medical and health information including condition or diagnosis, dates of service, patient account/record/ID numbers, (collectively, the "Private Information") from cybercriminals.

7. Gryphon provides Revenue cycle, coding and compliance, and consulting services for:

- Hospitals
- Emergency Departments and Physicians
- Ambulatory Surgery Centers
- Imaging Centers, Independent Labs
- Healthcare Facilities
- Large Physician Groups and Private Practices

8. EMS Services [1]

9. Plaintiff and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect against disclosure was targeted, compromised, and unlawfully accessed due to the Data Breach.

10. As part of its business, Defendant collects a treasure-trove of data from their clients, including highly sensitive Private Information.

11. Healthcare providers that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

[1] www.gryphonhc.com.

12. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters and other long-term issues.

13. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

14. Mitigating that risk requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

15. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

16. According to the Gryphon's own website, "recent data security incident that may have affected personal and/or protected health information. Gryphon takes the privacy and security of all information within its possession very seriously. (the "Data Breach").[2]

17. The breach involved the divulgence of Private Information of Defendant's clients including their: name, contact information (e.g., email address, phone number), date of birth, Social Security Number, government identification, and information about medical history and/or associated conditions, and/or unique identifiers to associate individuals with Gryphon.

[2] *See* www.gryphonhc.com/wp-conte:nt/uploads/2024/10/Data-Security-Incident.pdf.

18. According to a new release Gryphon Healthcare filed notice of third-party data breach affecting 393,358 people. *See* https://www.jdsupra.com/legalnews/gryphon-healthcare-files-notice-of-5757607/

19. The data could be used for malicious purposes in the wrong hands, such as phishing and social engineering.

20. A data breach is a type of cybersecurity intrusion whereby the cybercriminal deploys "ransomware" on a given entity's computer system and data storage network. Ransomware that works to "lock" access to a given computer system or data storage network until the entity pays a ransom, usually in untraceable cryptocurrency, in order to regain access.

21. Based on news reports Gryphon mounted an investigation into the breach itself, the causes, or what specific information of Plaintiff and the proposed Class was lost to criminals.

22. Defendant's "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

23. As a direct and proximate result of Defendant's failure to implement and to follow basic security procedures, Plaintiff's and Class Members' Private Information now appears to be in the hands of cybercriminals.

24. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, Private Information being disseminated on the dark web, and similar forms of criminal mischief, risk which may last for the rest of their lives.

25. Plaintiff and Class Members have also suffered concrete injuries in fact including, but not limited to, lost or diminished value of Private Information, lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, and actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails.

26. Consequently, Plaintiff and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

27. Plaintiff, on behalf of herself and all others similarly situated, therefore brings claims for (i) Negligence and Negligence *Per Se*; (ii) Implied Breach of Contract; (iii) Breach of Fiduciary Duty; (iv) Intrusion Upon Seclusion/Invasion of Privacy; (v) Unjust Enrichment and (vi) Declaratory Judgment and Injunctive Relief. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Plaintiff Sarah Smith

22. Plaintiff, Sarah Smith is, and at all times mentioned herein, an individual citizen residing in League City, Texas.

23. Plaintiff understandably and reasonably believed and trusted that Plaintiff's Private Information provided to Defendant would be kept confidential and secure and would be used only for authorized purposes.

Defendant Gryphon Healthcare, LLC

24. Defendant, Gryphon Healthcare is a foreign corporation, organized in Delaware with its headquarters in Texas. Its principal place of business is located at: 4700 W. Sam Houston Pkwy N #140, Houston, TX 77041.

25. According to the Defendant's website, Gryphon "The privacy and protection of personal and protected health information is a top priority for Gryphon."[3]

JURISDICTION & VENUE

26. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) in that (1) this action is a class action with more than a thousand (1,000) Class Members; (2) Defendant is a Texas Limited Liability Company, with its headquarters in Texas; (3) Plaintiff and members of the Class are citizens of the United States, thus satisfying the minimal diversity requirement of 28 U.S.C. § 1332(d)(2)(A); and (4) the matter in controversy exceeds the sum or value of $5,000,000 exclusive of interests and costs.

27. The acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

28. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District, and Defendant does business in this Judicial District.

[3] www.gryphonhc.com/wp-content/uploads/2024/10/Data-Security-Incident.pdf.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects a Significant Amount of Private Information.

29. Plaintiff and Class Members are current and former clients of Defendant.

30. Clients, including Plaintiff and Class Members, provided Defendant with their sensitive personally identifiable information and protected health information.

31. Upon information and belief, in the course of collecting Private Information from clients, including Plaintiff, Defendant promised to provide confidentiality and adequate security from the data it collected from clients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

32. Defendant states on its website that: "based on Gryphon's review, the following information for current and former patients may have been affected as a result of the incident: names, dates of birth, addresses, Social Security numbers, dates of service, diagnosis information, health insurance information, medical treatment information, prescription information, provider information and medical record number."[4]

33. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its clients, Defendant is required to keep clients' Private Information private; comply with industry standards related to data security and the maintenance of their clients' Private Information; inform their clients of its legal duties relating to data security; comply with all federal and state laws protecting clients' Private Information; only use and release clients' Private Information for reasons that relate to the services they provide; and provide adequate notice to clients if their Private Information is disclosed without authorization.

[4] www.gryphonhc.com/wp-content/uploads/2024/10/Data-Security-Incident.pdf.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

35. Without the required submission of Private Information from Plaintiff and Class Members, Defendant could not perform the services it provides.

36. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

37. Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiff's and Class Members' Private Information.

B. The Data Breach

39. On or about October 11, 2024, the Defendant's Data Breach was reported in the news media:

> "The company confirmed the news in a breach notification filed with the Office of the Maine Attorney General, stating a company partner that Gryphon provides medical billing services for was breached some time before August 13, 2024.".[5]

40. Other news sources stated:

> "Gryphon disclosed that infiltration of a customer's systems in August resulted in the exfiltration of personal and sensitive details from 393,358 patients, including names, birthdates, Social Security numbers, addresses, service dates, health insurance information, diagnoses, treatment and prescription details, medical record numbers, and provider information." [6]

---

[5] *See* https://www.msn.com/en-gb/health/other/medical-data-of-almost-400-000-americans-stolen-here-s-what-we-know/ar-AA1sk6qf.

[6] *See* https://www.scworld.com/brief/separate-health-breaches-impact-over-500k

41. Omitted from news sources is who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

42. Defendant has obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

43. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its clients' PII and PHI.

C. Defendant Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

44. Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

45. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

46. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless ones in the healthcare industry.

47. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[7]

48. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[8]

49. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

50. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[9]

51. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[10]

52. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now

---

[7] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited July 1, 2024).
[8] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcaredata-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited July 1, 2024).
[9] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://go.flashpointintel.com/docs/2021-Year-End-Report-data-breach-quickview (last visited July 1, 2024).
[10] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Sept. 15, 2024).

the biggest target for online attacks."[11]

53. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[12][13]

54. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

55. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[14]

56. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's clients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud and more.

57. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB,

---

[11] *9 Reasons Why Healthcare is the Biggest Target for Cyberattacks*, SWIVELSECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks (last visited Oct. 16, 2024).
[12] *Id.*
[13] *Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited July 1, 2024).
[14] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered337-healthcare-data-breaches-in-first-half-of-year.

Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[15]

58. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.[16] According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care,

coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[17]

---

[15] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[16] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PWC.COM (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[17] Brian O'Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one.

59. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

61. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

62. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[18] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

63. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

64. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

65. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

[18] *See* https://www.identitytheft.gov/Steps (last visited July 1, 2024).
[19] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 1, 2024).

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

66. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

67. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

68. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[21]

69. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-hasmillionsworrying-about-identity-theft.

[21] *Report to Congressional Requesters, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited July 1, 2024).

about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

70. Based on the value of its clients' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. The Data Breach was Preventable.

71. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

72. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

73. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented numerous measures as recommended by the United States Government, including but not limited to:

- Implementing an awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configuring firewalls to block access to known malicious IP addresses.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.
- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[22]

74. Given that Defendant was storing the Private Information of its current and former clients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

75. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiff and Class Members.

E. Defendant is Obligated Under HIPAA to Safeguard Private Information.

76. Defendant is required by HIPAA to safeguard patient PHI.

77. Defendant is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

78. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

79. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or

[22] How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 15, 2024).

PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

80. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

81. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

82. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[23]

83. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to

[23] U.S. Dep't of Health & Human Servs., *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breachnotification/index.html (last visited Sept. 15, 2024).

cybercriminals.

84. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

85. Given the application of HIPAA to Defendant, and that Plaintiff and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

86. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

87. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

88. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities,

[24] U.S. Fed. Trade Comm'n, *Start with Security – A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

and implement policies to correct any security problems.[25]

89. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

92. Defendant was at all times fully aware of its obligations to protect the PII and PHI of clients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[25] U.S. Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

G. Defendant Violated Industry Standards.

93. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Gryphon failed to follow these industry best practices, including a failure to implement multi-factor authentication.

94. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

95. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. The Monetary Value of Plaintiff's & Class Members' Private Information.

97. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

98. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[26]

99. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[27]

100. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[28]

101. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

102. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

The use of third-party information from public records, information aggregators and even

---

[26] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWB4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited July 1, 2024).

[27] *Id.*

[28] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[29]

103. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[30]

104. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[31]

105. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[32] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale

---

[29] U.S. Fed. Trade Comm'n, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Feb. 7, 2001), https://www.ftc.gov/legal-library/browse/federal-register-notices/public-workshop-information-marketplace-merging-exchanging-consumer-data.

[30] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[31] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploringprivacy-roundtable/091207privacyroundtable.pdf.

[32] Angwin & Steel, *supra* note 30.

and purchase of this valuable data.

106. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[33]

107. The value of Plaintiff's and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[34]

108. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

109. Health information, in particular, is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[35]

110. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to

---

[33] *See* U.S. Dep't of Justice, *Victims of Identity Theft* (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[34] *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector (last visited Sept. 15, 2024).
[35] *Id.*

their personal medical files due to the thief's activities."[36]

111. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiff's and Class Members' risk of suffering future medical identity theft is especially substantial.

112. The ramifications of Defendant's failure to keep its clients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

113. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[37]

114. Indeed, when compromised, healthcare-related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[38]

115. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data

---

[36] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft.

[37] *See Medical ID Theft Checklist*, https://www.identityforce.com/blog/medical-id-theftchecklist-2 (last visited July 6, 2024).

[38] Elinor Mills, *Study: Medical identity theft is costly for victims* (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims.

breaches and identity theft, including medical identity theft, have a crippling effect on individuals and detrimentally impact the economy as a whole.[39]

116. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

117. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of clients within their systems.

118. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

119. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[40] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[41]

120. Based upon information and belief, the unauthorized parties have already utilized,

---

[39] *Id.*

[40] U.S. Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38 (Dec. 2010), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[41] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that can be misused.

121. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

122. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

123. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

124. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

125. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

I. Plaintiff & Class Members Have Suffered Compensable Damages.

128. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

129. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to

thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

130. In order to mitigate against the risks of identity theft and fraud, Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

131. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

132. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

133. Plaintiff and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

134. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its clients' PII and PHI.

135. Plaintiff and Class Members have suffered emotional distress because of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

136. Plaintiff and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

137. Plaintiff and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

138. Finally, in addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

Plaintiff Sarah Smith

139. Plaintiff, Sarah Smith used the services of Defendant for medical billing.

140. As a condition of obtaining services from Defendant, she was required to provide her Private Information to Defendant.

141. Upon information and good faith belief, Defendant maintained Plaintiff's Private Information in its systems at the time of the Data Breach.

142. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff's stores any documents containing Plaintiff's Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted Plaintiff's Private Information to Defendant had she known of Defendant's lax data security policies.

143. As a result of the Data Breach, Plaintiff's made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. On October 15, 2024, Plaintiff receive a letter from Defendant placing her on notice that she was part of the Data Breach.

145. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so

long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

146. Plaintiff additionally suffered actual injury in the form of her Private Information being disseminated, on information and belief, on the dark web as a result of the Data Breach.

147. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

148. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

149. Plaintiff, Sarah Smith has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

150. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

151. Specifically, Plaintiff proposes the following class definitions, subject to amendment as appropriate:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised in the Data Breach with Gryphon Healthcare, LLC on or before August 13, 2024 (the "Nationwide Class").

152. Excluded from the Classes are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect

of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

153. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

154. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes many thousands of individuals, if not substantially more.

155. **Commonality:** This action involved questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

c. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiff and Class Members for non-business purposes;

e. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and

Class Members;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

l. Whether Defendant was negligent and that negligence resulted in the Data Breach;

m. Whether Defendant entered into an implied contract with Plaintiff and Class Members;

n. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and Class Members' PII and PHI;

o. Whether Defendant were unjustly enriched;

p. Whether Plaintiff and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

q. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

156. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all clients, or family members or caregivers of clients, of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

157. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

158. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

159. **Superiority and Manageability:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and

provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

160. Class action Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

161. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

162. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

163. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

164. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

165. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

166. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

167. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

168. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class.

169. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

FIRST COUNT -NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and all Class Members)

170. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

171. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff's and Class Members' PHI/PII on its computer systems and networks.

172. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession;

b. to protect Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

173. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

174. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches. 91. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI/PII.

175. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Plaintiff and Class Members had entrusted to it.

176. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI/PII.

177. Because Defendant knew that a breach of its systems could damage hundreds of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained thereon.

178. Plaintiff's and Class Members' willingness to entrust Defendant with its PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

179. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiff and/or the remaining Class Members.

180. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiff's and Class

Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

181. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

182. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

183. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PHI/PII and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members. Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

184. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

185. The damages Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

186. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

187. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

188. Similarly, HIPAA provides a clear, prescriptive requirement for Defendant to implement certain cybersecurity safeguards, which Defendant failed to do. *See* 45 C.F.R. Pt. 164.

189. Defendant's violations of 15 U.S.C. § 45 constitutes negligence *per se.* Defendant also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*, as these requirements were designed to protect consumers from the harms inherent in the exposure of their personal information, including PII and PHI.

190. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data

Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

191. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

192. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession.

SECOND COUNT – IMPLIED BREACH OF CONTRACT
(On Behalf of Plaintiff and all Class Members)

193. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

194. When Plaintiff and Class Members provided their PII and PHI to Defendant in exchange for a medical services and treatment, they entered into implied contracts and they did so with the belief that Defendant had agreed to reasonably protect such information.

195. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

196. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

197. Plaintiff and Class Members provided services to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so. Class Members similarly paid money to Defendant for its services with the reasonable belief and expectation that Defendant would use part of that payment to obtain adequate data security for the PII consumers entrusted to Defendant. Defendant failed to do so.

198. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

199. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

200. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

201. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

202. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

203. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

204. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT - BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

205. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

206. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became health care providers of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and heighten relationship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

207. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them, in particular, to keep secure their PII.

208. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate the Data Breach in a reasonable and practicable period.

209. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

210. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

211. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

212. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FOURTH COUNT - INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

213. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

214. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.
>
> Restatement (Second) of Torts§ 652B (1977).

215. Plaintiff and Class Members had a reasonable expectation of privacy in the PII and PHI that Defendant mishandled.

216. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

217. By intentionally failing to keep Plaintiff's and Class Members' PII and PHI safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

> a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;
>
> b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and
>
> c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

218. Indeed, given the foreseeability of the harms inherent in data breaches and the ubiquitous nature of data breaches, Defendant was substantially certain that its failure to implement reasonable cybersecurity standards would lead to an invasion of Plaintiff's privacy.

219. Defendant knew that an ordinary person in Plaintiff or Class Members' position would consider the exposure of their PII and PHI to be highly offensive and objectionable.

220. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their PII and PHI without their informed, voluntary, affirmative, and clear consent.

221. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their PII and PHI without their informed, voluntary, affirmative, and clear consent.

222. Moreover, given that stolen PII and PHI is then publicized and traded on the dark web and through Telegram channels, Defendant knew or was substantially certain that its failure to implement reasonable cybersecurity safeguards would lead to the publication of Plaintiff's and the Class Members' PII and PHI to a large group of the public and/or to a large group of individuals who are in a special relationship with Plaintiff and the proposed Class Members, in that those individuals are exactly the type of people that Plaintiff and the Class Members have a special interest in ensuring their PII and PHI is kept confidential from given that those individuals are known identity thieves and fraudsters.

223. The conduct described above was at or directed at Plaintiff and the Class Members.

224. As a proximate result of such intentional misuse and disclosures, Plaintiff and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class

Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

225. In failing to protect Plaintiff's and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

FIFTH COUNT - IN THE ALTERNATIVE - UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

226. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

227. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count, the third count listed in this Complaint.

228. Representative Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its clients and in so doing also provided Defendant with their Private Information. In exchange, Representative Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

229. Defendant knew that Representative Plaintiff and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Representative Plaintiff and Class Members for business purposes.

230. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Representative Plaintiff and Class Members.

231. As such, a portion of the payments made for the benefit of or on behalf of Representative Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

232. Defendant, however, failed to secure Representative Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Representative Plaintiff and Class Members provided.

233. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Representative Plaintiff and Class Members and derived revenue by using it for business purposes. Representative Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

234. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

235. If Representative Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

236. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Representative Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the

hacking incident, Defendant instead calculated to increase its own profit at the expense of Representative Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Representative Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

237. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Representative Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

238. Representative Plaintiff and Class Members have no adequate remedy at law.

239. As a direct and proximate result of Defendant's conduct, Representative Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

240. As a direct and proximate result of Defendant's conduct, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

241. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Representative Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

SIXTH COUNT - DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and All Class Members)

242. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 169.

243. Plaintiff brings this claim individually and on behalf of the Class.

244. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

245. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

246. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

247. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

248. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

249. The risk of another such breach is real, immediate and substantial.

250. If another breach of Defendant's store of patient data occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

251. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

139. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant [what], thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

JURY TRIAL DEMANDED

140. Plaintiff demands a trial by jury on all claims so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court

reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. Prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 5 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded at the prevailing legal rate; and

K. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and other members of the proposed Classes, hereby demands a jury trial on all issues so triable.

Dated: October 16, 2024

Respectfully submitted,

/s/ *T. J. Jesky*

T. J. Jesky
LAW OFFICES OF T. J. JESKY
205 N. Michigan Avenue, Suite 810
Chicago, IL 60601-5902
tj@jeskylaw.com
Telephone: 312-894-0130, Ext. 3
Fax: 312-489-8216

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Grayson Wells (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Phone: (615) 254-8801
gstranch@stranchlaw.com

Counsel for Plaintiff and the Proposed Class Members